REMARKS

Claims 1-8, 15, and 16 are pending. Claims 1 and 15 are amended. Claims 9-14 are canceled without prejudice or disclaimer to be filed at a later date.

The claim amendments are supported by the application as originally filed, for example, on pages 36-37, paragraphs 1145-1147. No new matter has been added.

Claim Rejections – 35 U.S.C. § 112

Claims 1, 9, and 10 were rejected under 35 U.S.C. § 112 as lacking proper antecedent basis for "the identity."

Claim 1 has been amended for other reasons and without prejudice or disclaimer to remove the term, "the identity." Claims 9 and 10 have been canceled for other reasons and without prejudice or disclaimer to be filed at a later date. Reconsideration is respectfully requested.

Claim Rejections – 35 U.S.C. § 101

Claims 9 and 10-14 were rejected under 35 U.S.C. § 101 as unpatentable subject matter. While Applicant disagrees with this rejection, for the reasons set forth in the last Amendment filed April 25, 2007, the claims at issue have been canceled without prejudice or disclaimer to be filed at a later date, to expedite prosecution of the present application.

Claim Rejections – 35 U.S.C. § 103

Claims 9-14

Claims 9-14 were rejected under 35 U.S.C. § 103(a) as obvious in view of U.S. Patent No. 6,704,768 to Zombek et al. (Zombek) and U.S. Patent No. 7,088,727 to Short et al. (Short).

Claims 9-14 have been canceled without prejudice or disclaimer to be filed at a later date. Accordingly, Applicant respectfully submits that this rejection is moot. Reconsideration is respectfully requested.

Claims 1-8

Claims 1-8 were rejected under 35 U.S.C. § 103(a) as obvious in view of Zombek, Short, U.S. Patent Application Publication 20010005358 (hereinafter Shiozawa), and Official Notice. The Applicant respectfully requests reconsideration for the following reasons.

Claim 1, as amended, defines a method for routing a message between services in a message routing network, including the features of:

> **(a) associating an identifier with an entity that has been authenticated by said message routing network, wherein said identifier is to be associated with an entity account upon authentication of said entity with a first service that supports said entity account;**
>
> (b) receiving, from a second service, a message including said identifier, said message being directed to a mapped service, wherein said mapped service is an entity account-specific representation of said first service and acts as a proxy for said first service, and wherein said mapped service is operable to determine whether a route for said message needs to be modified prior to delivering said message to said first service;
>
> **(c) authenticating said message routing network using said identifier included in said message; and**
>
> **(d) when said message routing network is authenticated using said identifier** and said mapped service determines that said route for said message does not need to be modified, **translating, by said message routing network, said message for delivery to said first service,** wherein said translated message includes said identifier and is directed from said mapped service to said first service.
>
> (Emphasis added).

In embodiments of the method defined in claim 1, the message interchange network authenticates each service that participates in a message's route. The message interchange

network can then provide an identifier, such as an authentication token, that substitutes for an enterprise's authentication credentials. The token is an identifier such as a GCID that represents an authenticated service to the enterprise's account with a specific service, such as an ASP. Thus, for instance, an ASP that receives a GCID in a message only needs to authenticate the message interchange network, since the message interchange network has already authenticated the message sender. (Application as originally filed, paragraph 1145).

Zombek describes message routers (MRs), which are capable of determining that the message sender is an authorized customer of an intelligent message network. (col. 21, lines 32-34). However, Zombek teaches that the MR authenticates the client device 112, which originally sent the message, rather than authenticate the message network, using an identifier included in the message. Zombek fails to disclose or suggest the possibility of authenticating the message network using an identifier in the message, as defined in claim 1.

In particular, Zombek fails to disclose or suggest at least several features recited in claim 1, including "(a) associating an identifier with an entity that has been authenticated by said message routing network, wherein said identifier is to be associated with an entity account upon authentication of said entity with a first service that supports said entity account;" "(c) authenticating said message routing network using said identifier included in said message;" and "(d) when said message routing network is authenticated using said identifier . . ., translating, by said message routing network, said message for delivery to said first service."

Instead, Zombek suggests that the MR 124 use the client device's source address (e.g., IP address or Mobitex MAN number) as the means of identifying authorized access. (col. 21, lines 35-38). Thus, for each client message the MR receives, the MR has to check the device address against a local cache of authorized devices 112, and additional databases. (col. 21, lines 39-41). The method of claim 1, on the other hand, provides for "associating an identifier with an entity that has been authenticated by the message routing network, wherein said identifier is to be

associated with an entity account upon authentication of said entity with a first service that supports said entity account." (Emphasis added). Nowhere does Zombek disclose or suggest that such the client device address also serve as, or be replaced by, an identifier associated with an entity that has been authenticated by a message routing network, as provided in claim 1.

Further, in Zombek, after checking the client device address for the message, Zombek teaches that if the device address is an authorized client device 12, and other conditions are satisfied, the message can be considered authentic and forwarded to the proper BES 122. (col. 21, lines 42-51). In claim 1, because the entity has already been authenticated, the method further includes the feature of "authenticating said message routing network using said identifier included in said message," as recited in element (c). (Emphasis added). Thus, for instance, in embodiments of claim 1, an ASP that receives an identifier in a message only needs to authenticate the message routing network, since the message sender has already been authenticated by the message routing network. There is no passage in Zombek that discloses or suggests that an identifier as defined in claim 1 be used to authenticate a message routing network, instead of the client device.

Applicant disagrees that those of ordinary skill in the art had any reason to combine Short with Zombek, at the time of the present invention, to arrive at the method of claim 1. Nonetheless, Short would fail to cure the deficiencies of Zombek even if such a reason existed. Short fails to disclose or suggest any authentication process or techniques. While Short describes a processor capable of intercepting a message and translating the data (col. 2, lines 20-22), nothing in Short describes or suggests that the processor or other mechanism authenticate the message, much less do anything corresponding to "(a) associating an identifier with an entity that has been authenticated by said message routing network, wherein said identifier is to be associated with an entity account upon authentication of said entity with a first service that supports said entity account;" "(c) authenticating said message routing network using said

identifier included in said message;" or "(d) when said message routing network is authenticated using said identifier . . ., translating, by said message routing network, said message for delivery to said first service," as recited in claim 1.

Shiozawa and the Official Notice similarly fail to cure Zombek in this regard. Again, Applicant disagrees that any reason existed to combine Shiozawa and the Official Notice with Zombek and Short, at the time of the present invention, to arrive at the method of claim 1. Nonetheless, if there were such a reason, Shiozawa's described packet protection techniques include no mention of authentication processes or techniques, such as "(a) associating an identifier with an entity that has been authenticated by said message routing network, wherein said identifier is to be associated with an entity account upon authentication of said entity with a first service that supports said entity account;" "(c) authenticating said message routing network using said identifier included in said message;" or "(d) when said message routing network is authenticated using said identifier . . ., translating, by said message routing network, said message for delivery to said first service," as recited in claim 1. There is simply no passage in Shiozawa that discloses or remotely suggests such authentication techniques. The Official Notice has nothing to do with authentication techniques, and does not address authenticating message routing networks, using identifiers included in the message or otherwise.

Because Short, Shiozawa, and the Official Notice fail to disclose or suggest the same claimed features lacking in Zombek, the cited references fail to support the obviousness rejection of claim 1, considered alone or in combination under 35 U.S.C. § 103(a). Accordingly, this rejection should be withdrawn.

Claims 2-8 are dependent upon claim 1 and are, therefore, patentable for at least the same reasons as claim 1. Applicant submits that claims 2-8 may also be separately patentable for additional reasons.

Claims 15-16

Claim 15 has been amended to recite similar features as claim 1 and is, therefore, neither anticipated by nor obvious in view of Zombek, Short, Shiozawa, and the Official Notice, considered alone or in combination, for similar reasons as described above.

In addition, claims 15 and 16 were rejected under 35 U.S.C. § 103(a) as being obvious in view of U.S. Patent Application Publication 2004/0243574 to Giroux et al. (Giroux), U.S. Patent No. 6,925,488 to Bantz et al. (Bantz), and Zombek. The Applicant respectfully requests withdrawal of these rejections for the following reasons.

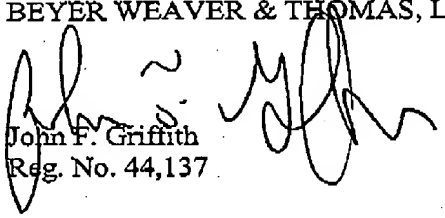
Giroux and Bantz fail to cure Zombek with respect to the same lacking features described above. For instance, Giroux's data replication methods include no mention of authentication processes or techniques, such as "(d) authenticating said message routing network using said identifier included in said message;" or "(e) when said message routing network is authenticated using said identifier, translating, by said message routing network, said message for delivery to said first service," as recited in claim 15. There is simply no passage in Giroux that discloses or remotely suggests such authentication techniques. Similarly, Bantz teaches distribution of system management messages, but fails to disclose or suggest authentication techniques, such as those described above. Bantz offers no teaching or suggestion of authenticating message routing networks using identifiers included in messages.

Because Giroux and Bantz fail to disclose or suggest the same claimed features lacking in Zombek, the cited references fail to support the obviousness rejection of claims 15 and 16, considered alone or in combination under 35 U.S.C. § 103(a). Accordingly, this rejection should also be withdrawn.

Conclusion

The Applicant believes that all pending claims are allowable and respectfully request a Notice of Allowance for this application from the Examiner. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP



John F. Griffith
Reg. No. 44,137

P.O. Box 70250
Oakland, CA 94612-0250
(650) 961-8300